

# Cisco Secure Firewall ASA シリーズ 9.19(x) リリースノート

初版：2022 年 11 月 29 日

最終更新：2024 年 4 月 25 日

## Cisco Secure Firewall ASA シリーズ 9.19(x) リリースノート

このドキュメントには、ASA ソフトウェアバージョン 9.19(x) のリリース情報が記載されています。

### 特記事項

- Firepower 4110、4120、4140、4150 に対する ASA 9.19(1) 以降のサポート、および Firepower 9300 に対するセキュリティモジュール SM-24、SM-36、SM-44 のサポートはありません。ASA 9.18(x) がサポートされている最後のバージョンです。

### システム要件

ASDM には、4 コア以上の CPU を搭載したコンピュータが必要です。コア数が少ないと、メモリ使用量が高くなる可能性があります。

### ASA と ASDM の互換性

ASA/ASDM ソフトウェアおよびハードウェアの要件およびモジュールの互換性を含む互換性の詳細については、『[Cisco Secure Firewall ASA Compatibility](#)』を参照してください。

### VPN の互換性

VPN の互換性については、『[Supported VPN Platforms, Cisco ASA 5500 Series](#)』を参照してください。

### 新機能

このセクションでは、各リリースの新機能を示します。



(注) syslog メッセージガイドに、新規、変更済み、および廃止された syslog メッセージを記載しています。

## ASA 9.19(1) の新機能

リリース日：2022 年 11 月 29 日

| 機能   | 説明  |
|--|---|
| <b>プラットフォーム機能</b>                                  |   |
| Cisco Secure Firewall 3105                         | Cisco Secure Firewall 3105 の ASA を導入しました。   |
| Azure ゲートウェイロードバランサを使用した ASA Virtual 自動スケールソリューション | Microsoft Azure にゲートウェイロードバランサを使用して ASA Virtual 自動スケールソリューションを展開できます。詳細については、インターフェイス機能を参照してください。   |
| <b>ファイアウォール機能</b>                                  |   |
| ネットワークサービスグループのサポート                                | 最大 1024 のネットワーク サービス グループを定義できるようになりました。  |
| <b>ハイアベイラビリティとスケラビリティの各機能</b>                      |   |
| バイアス言語の除去  | 「Master」と「Slave」という用語を含むコマンド、コマンド出力、syslog メッセージは、「Control」と「Control」に変更されました。<br><br>新規/変更されたコマンド： <b>cluster control-node</b> 、 <b>enable as-data-node</b> 、 <b>prompt</b> 、 <b>show cluster history</b> 、 <b>show cluster info</b> |
| ASA Virtual Amazon Web Services (AWS) クラスターリング     | ASA Virtual は AWS で最大 16 ノードの個別インターフェイスのクラスターリングをサポートします。AWS ゲートウェイロードバランサの有無にかかわらず、クラスターリングを使用できます。  |
| <b>ルーティング機能</b>                                    |   |
| IPv6 の BGP グレースフルリスタート                             | IPv6 アドレスファミリの BGP グレースフルリスタートサポートを追加しました。<br><br>新規/変更されたコマンド：IPv6 ファミリをサポートするために拡張された既存のコマンド： <b>ha-mode graceful-restart</b>   |
| <b>インターフェイス機能</b>                                  |   |

| 機能  | 説明  |
|---|---|
| ASA Virtual で IPv6 をサポート  | <p>ASAv は、プライベートおよびパブリック クラウドプラットフォームで IPv6 ネットワークプロトコルをサポートします。</p> <p>ユーザーは次のことができるようになりました。</p> <ul style="list-style-type: none"> <li>• day0 設定で IPv6 管理アドレスを有効にして構成します。</li> <li>• DHCP および静的な方法を使用して IPv6 アドレスを割り当てます。</li> </ul>   |
| Azure ゲートウェイロードバランサの ASA Virtual のペアプロキシ VXLAN  | <p>Azure ゲートウェイ ロードバランサ (GWL) で使用するために、Azure の ASA Virtual のペアプロキシモード VXLAN インターフェイスを構成できます。ASA Virtual は、ペアプロキシの VXLAN セグメントを利用して、単一の NIC に外部インターフェイスと内部インターフェイスを定義します。</p> <p>新規/変更されたコマンド：<b>external-port</b>、<b>external-segment-id</b>、<b>internal-port</b>、<b>internal-segment-id</b>、<b>proxy paired</b></p>                |
| Secure Firewall 3100 固定ポートのデフォルトの前方誤り訂正 (FEC) が、25 GB+ SR、CSR、および LR トランシーバの cl74-fc から cl108-rs に変更されました | <p>Secure Firewall 3100 の固定ポートで FEC を Auto に設定すると、25 GB SR、CSR、および LR トランシーバのデフォルトのタイプが cl74-fc ではなく cl108-rs に設定されるようになりました。</p> <p>新規/変更されたコマンド：<b>fec</b></p>  |
| <b>ライセンス機能</b>  |   |
| KVM および VMware 上の ASAv5 の ASA Virtual 永久ライセンス予約のサポート  | <p>デフォルトの PLR ソフトウェア利用資格を上書きし、KVM および VMware に 2GB RAM の ASAv を展開するときに Cisco Smart Software Manager (SSM) に ASAv5 PLR ライセンスを発行するように要求する新しいコマンドを利用できます。RAM の設定に合わせてソフトウェア利用資格を ASAv5 からデフォルトの PLR ライセンスに戻すための &lt;no&gt; 形式を追加することにより、このコマンドを変更できます。</p>   |
| <b>管理、モニタリング、およびトラブルシューティングの機能</b>  |   |
| CiscoSSH スタックのデフォルト化  | <p>Cisco SSH スタックがデフォルトで使用されるようになりました。</p> <p>新規/変更されたコマンド：<b>ssh stack ciscossh</b></p>  |
| <b>VPN 機能</b>   |   |
| VTI ループバック インターフェイスのサポート  | <p>ループバック インターフェイスを VTI の送信元インターフェイスとして設定できるようになりました。静的に設定された IP アドレスの代わりに、ループバック インターフェイスから IP アドレスを継承するサポートも追加されました。ループバック インターフェイスは、パス障害の克服に役立ちます。インターフェイスがダウンした場合、ループバック インターフェイスに割り当てられた IP アドレスを使用してすべてのインターフェイスにアクセスできます。</p> <p>新規/変更されたコマンド：<b>tunnel source interface</b>、<b>ip unnumbered</b>、<b>ipv6 unnumbered</b></p> |

| 機能  | 説明  |
|---|---|
| ダイナミック仮想トンネルインターフェイス（ダイナミック VTI）のサポート     | <p>ダイナミック VTI により ASA が強化されました。ハブの複数のスタティック VTI 構成を単一のダイナミック VTI に置き換えることができます。ハブの構成を変更せずに、新しいスポークをハブに追加できます。ダイナミック VTI はダイナミック（DHCP）スポークをサポートします。</p> <p>新規/変更されたコマンド：<b>interface virtual-Template、ip unnumbered、ipv6 unnumbered、tunnel protection ipsec policy</b></p>   |
| EIGRP および OSPF の VTI サポート                 | <p>EIGRP および OSPFv2/v3 ルーティングが仮想トンネルインターフェイスでサポートされるようになりました。これらのルーティングプロトコルを使用して、ルーティング情報を共有し、ピア間の VTI ベースの VPN トンネルを介してトラフィックフローをルーティングできます。</p>  |
| リモートアクセス VPN の TLS 1.3                    | <p>TLS 1.3 を使用して、リモートアクセス VPN 接続を暗号化できます。</p> <p>TLS 1.3 では、次の暗号方式のサポートが追加されています。</p> <ul style="list-style-type: none"> <li>• TLS_AES_128_GCM_SHA256</li> <li>• TLS_CHACHA20_POLY1305_SHA256</li> <li>• TLS_AES_256_GCM_SHA384</li> </ul> <p>この機能には、Cisco Secure Client バージョン 5.0.01242 以降が必要です。</p> <p>新規/変更されたコマンド：<b>sslserver-version、sslclient-version</b></p>  |
| IKEv2 サードパーティクライアントのデュアルスタックサポートが追加されました。 | <p>Cisco Secure Firewall ASA は、IKEv2 サードパーティのリモートアクセス VPN クライアントからのデュアルスタック IP 要求をサポートするようになりました。サードパーティのリモートアクセス VPN クライアントが IPv4 アドレスと IPv6 アドレスの両方を要求した場合、ASA は、複数のトラフィックセクタを使用して両方の IP バージョンアドレスを割り当てることができます。この機能により、サードパーティのリモートアクセス VPN クライアントは、単一の IPsec トンネルを使用して IPv4 および IPv6 データトラフィックを送信できます。</p> <p>新規/変更されたコマンド：<b>show crypto ikev2 sa、show crypto ipsec sa、show vpn-sessiondb ra-ikev2-ipsec</b></p> |
| スタティック VTI インターフェイスのトラフィックセクタ             | <p>スタティック VTI インターフェイスのトラフィックセクタを割り当てることができるようになりました。</p> <p>新規/変更されたコマンド：<b>tunnel protection ipsec policy</b></p>   |

## ソフトウェアのアップグレード

このセクションには、アップグレードを完了するためのアップグレードパス情報とリンクが記載されています。

## ASA のアップグレードパス

現在のバージョンとモデルを表示するには、次のいずれかの方法を使用します。

- ASDM : [Home] > [Device Dashboard] > [Device Information] の順に選択します。
- CLI : `show version` コマンドを使用します。

次の表に、ASA のアップグレードパスを示します。バージョンによっては、新しいバージョンにアップグレードする前に、中間アップグレードが必要な場合があります。推奨バージョンは太字で示されています。



- (注) 開始バージョンと終了バージョンの間で、各リリースのアップグレードガイドラインを必ず確認してください。場合によっては、アップグレードする前に構成を変更する必要があります。そうしないと、停止が発生する可能性があります。



- (注) ASA のセキュリティの問題と、各問題に対する修正を含むリリースについては、[ASA Security Advisories](#) を参照してください。



- (注) 9.18 は Firepower 4110、4120、4140、4150、および Firepower 9300 のセキュリティモジュール SM-24、SM-36、SM-44 の最終バージョンです。
- ASA 9.16 は ASA 5506-X、5508-X、および 5516-X の最終バージョンです。
- ASA 9.14 は ASA 5525-X、5545-X、および 5555-X の最終バージョンです。
- ASA 9.12 は ASA 5512-X、5515-X、5585-X、および ASASM 用の最終バージョン、
- ASA 9.2 は ASA 5505 の最終バージョンです。
- ASA 9.1 は ASA 5510、5520、5540、5550、および 5580 の最終バージョンです。

| 現在のバージョン | 暫定アップグレードバージョン | ターゲットバージョン                                     |
|----------|----------------|--|
| 9.18     | —              | 次のいずれかになります。<br>→ <b>9.19</b>                  |
| 9.17     | —              | 次のいずれかになります。<br>→ <b>9.19</b><br>→ <b>9.18</b> |

| 現在のバージョン | 暫定アップグレードバージョン | ターゲットバージョン  |
|----------|----------------|---|
| 9.16     | —              | 次のいずれかになります。<br>→ <b>9.19</b><br>→ <b>9.18</b><br>→ 9.17                                      |
| 9.15     | —              | 次のいずれかになります。<br>→ <b>9.19</b><br>→ <b>9.18</b><br>→ 9.17<br>→ <b>9.16</b>                     |
| 9.14     | —              | 次のいずれかになります。<br>→ <b>9.19</b><br>→ <b>9.18</b><br>→ 9.17<br>→ <b>9.16</b><br>→ 9.15           |
| 9.13     | —              | 次のいずれかになります。<br>→ <b>9.19</b><br>→ <b>9.18</b><br>→ 9.17<br>→ <b>9.16</b><br>→ 9.15<br>→ 9.14 |
| 9.12     | —              | 次のいずれかになります。<br>→ <b>9.19</b><br>→ <b>9.18</b><br>→ 9.17<br>→ <b>9.16</b><br>→ 9.15<br>→ 9.14 |

| 現在のバージョン | 暫定アップグレードバージョン | ターゲットバージョン  |
|----------|----------------|---|
| 9.10     | —              | 次のいずれかになります。<br>→ <b>9.19</b><br>→ <b>9.18</b><br>→ 9.17<br>→ <b>9.16</b><br>→ 9.15<br>→ 9.14<br>→ 9.12 |
| 9.9      | —              | 次のいずれかになります。<br>→ <b>9.19</b><br>→ <b>9.18</b><br>→ 9.17<br>→ <b>9.16</b><br>→ 9.15<br>→ 9.14<br>→ 9.12 |
| 9.8      | —              | 次のいずれかになります。<br>→ <b>9.19</b><br>→ <b>9.18</b><br>→ 9.17<br>→ <b>9.16</b><br>→ 9.15<br>→ 9.14<br>→ 9.12 |

| 現在のバージョン | 暫定アップグレードバージョン | ターゲットバージョン   |
|----------|----------------|--|
| 9.7      | —              | 次のいずれかになります。<br>→ <b>9.19</b><br>→ <b>9.18</b><br>→ 9.17<br>→ <b>9.16</b><br>→ 9.15<br>→ 9.14<br>→ 9.12<br>→ 9.8 |
| 9.6      | —              | 次のいずれかになります。<br>→ <b>9.19</b><br>→ <b>9.18</b><br>→ 9.17<br>→ <b>9.16</b><br>→ 9.15<br>→ 9.14<br>→ 9.12<br>→ 9.8 |
| 9.5      | —              | 次のいずれかになります。<br>→ <b>9.19</b><br>→ <b>9.18</b><br>→ 9.17<br>→ <b>9.16</b><br>→ 9.15<br>→ 9.14<br>→ 9.12<br>→ 9.8 |



| 現在のバージョン | 暫定アップグレードバージョン | ターゲットバージョン   |
|----------|----------------|--|
| 9.4      | —              | 次のいずれかになります。<br>→ <b>9.19</b><br>→ <b>9.18</b><br>→ 9.17<br>→ <b>9.16</b><br>→ 9.15<br>→ 9.14<br>→ 9.12<br>→ 9.8 |
| 9.3      | —              | 次のいずれかになります。<br>→ <b>9.19</b><br>→ <b>9.18</b><br>→ 9.17<br>→ <b>9.16</b><br>→ 9.15<br>→ 9.14<br>→ 9.12<br>→ 9.8 |
| 9.2      | —              | 次のいずれかになります。<br>→ <b>9.19</b><br>→ <b>9.18</b><br>→ 9.17<br>→ <b>9.16</b><br>→ 9.15<br>→ 9.14<br>→ 9.12<br>→ 9.8 |

| 現在のバージョン  | 暫定アップグレードバージョン | ターゲットバージョン  |
|---|----------------|---|
| 9.1(2)、9.1(3)、9.1(4)、9.1(5)、9.1(6)、または 9.1(7.4) | —              | 次のいずれかになります。<br>→ 9.14<br>→ <b>9.12</b><br>→ 9.8<br>→ 9.1(7.4)          |
| 9.1(1)  | → 9.1(2)       | 次のいずれかになります。<br>→ 9.14<br>→ <b>9.12</b><br>→ 9.8<br>→ 9.1(7.4)          |
| 9.0(2)、9.0(3)、または 9.0(4)                        | —              | 次のいずれかになります。<br>→ 9.14<br>→ <b>9.12</b><br>→ 9.8<br>→ 9.6<br>→ 9.1(7.4) |
| 9.0(1)  | → 9.0(4)       | 次のいずれかになります。<br>→ 9.14<br>→ <b>9.12</b><br>→ 9.8<br>→ 9.1(7.4)          |
| 8.6(1)  | → 9.0(4)       | 次のいずれかになります。<br>→ 9.14<br>→ <b>9.12</b><br>→ 9.8<br>→ 9.1(7.4)          |

| 現在のバージョン        | 暫定アップグレードバージョン | ターゲットバージョン   |
|-----------------|----------------|--|
| 8.5(1)          | → 9.0(4)       | 次のいずれかになります。<br>→ <b>9.12</b><br>→ 9.8<br>→ 9.1(7.4)             |
| 8.4(5+)         | —              | 次のいずれかになります。<br>→ <b>9.12</b><br>→ 9.8<br>→ 9.1(7.4)<br>→ 9.0(4) |
| 8.4(1) ~ 8.4(4) | → 9.0(4)       | → <b>9.12</b><br>→ 9.8<br>→ 9.1(7.4)                             |
| 8.3             | → 9.0(4)       | 次のいずれかになります。<br>→ <b>9.12</b><br>→ 9.8<br>→ 9.1(7.4)             |
| 8.2 以前          | → 9.0(4)       | 次のいずれかになります。<br>→ <b>9.12</b><br>→ 9.8<br>→ 9.1(7.4)             |

## アップグレードリンク

アップグレードを完了するには、『[ASA アップグレードガイド](#)』を参照してください。

## 未解決のバグおよび解決されたバグ

このリリースで未解決のバグおよび解決済みのバグには、Cisco Bug Search Tool を使用してアクセスできます。この Web ベースツールから、この製品やその他のシスコハードウェアおよびソフトウェア製品でのバグと脆弱性に関する情報を保守するシスコバグトラッキングシステムにアクセスできます。



- (注) Cisco Bug Search Tool にログインしてこのツールを使用するには、Cisco.com アカウントが必要です。アカウントがない場合は、[アカウントを登録](#)できます。シスコサポート契約がない場合は、ID でのみバグを探ることができます。検索は実行できません。

Cisco Bug Search Tool の詳細については、[Bug Search Tool Help & FAQ \[英語\]](#) を参照してください。

## バージョン 9.19(x) で未解決のバグ

次の表に、このリリースノートの発行時点で未解決のバグを示します。

| ID                         | 見出し   |
|----------------------------|---|
| <a href="#">CSCwc58458</a> | AWS C5N-4Xlarge 10g インターフェイスに、GENEVE とジャンボフレームが有効になっている 4 つの RX キューしかない |

## バージョン 9.19(1) で解決済みのバグ

次の表に、このリリースノートの発行時点で解決済みのバグを示します。

| ID                         | 見出し   |
|----------------------------|---|
| <a href="#">CSCvv82681</a> | RTC の不安定なクロックレジスタ読み取りにより、コンソールで「ウォッチドッグ：バグ：ソフトロックアップ-CPU#0がスタック (watchdog: BUG: soft lockup - CPU#0 stuck)」エラーが発生する |
| <a href="#">CSCvw23514</a> | 潜在的な SSD HW 障害の切り分けに関する詳細を提供するために、FXOS トラブルシューティング マニュアルを更新   |
| <a href="#">CSCvx54562</a> | FTD の高いシステムオーバーヘッドのメモリ  |
| <a href="#">CSCvx99172</a> | 4100/9300 上の M500IT モデルのソリッドステートドライブが 3 年 2 カ月のサービス期間後に応答しなくなることがある   |
| <a href="#">CSCvy99348</a> | shutdown コマンドが、FP1k デバイスをシャットダウンする代わりに再起動する   |
| <a href="#">CSCvz34289</a> | 場合によっては、軽量プロキシへの移行が Do Not Decrypt フローで機能しない  |
| <a href="#">CSCvz52785</a> | 9.12 から 9.14.2.15 へのアップグレード後、管理インターフェイスが 13 分ごとにフラップする  |
| <a href="#">CSCvz68713</a> | ASAv5 の PLR ライセンス予約は ASAv10 を要求している   |
| <a href="#">CSCvz69729</a> | 不安定なクライアントプロセスは、FTD で LINA zmqio トレースバックを引き起こす可能性がある  |

| ID         | 見出し  |
|------------|--|
| CSCVz90712 | 9.17/レア 256 ブロックのリーク/枯渇、1550 ブロックの割り当て超過   |
| CSCVz94217 | アプリケーションインスタンスの起動バージョンを無視し、設定のコピー後に実行バージョンに設定する  |
| CSCwa16257 | ループバック インターフェイスが設定されている場合に、フェールオーバーがセカンダリ FTD で失敗する  |
| CSCwa38996 | snmpd.log leading で大量のメッセージが繰り返されてログサイズが大きくなる  |
| CSCwa48169 | netsnmp_handler_check_cache 関数での ASA/FTD のトレースバックとリロード   |
| CSCwa52215 | ファームウェアをアップロードすると、データポートチャネルがフラッピングする  |
| CSCwa55772 | FPR 4100 では、「リセットの HA ポリシーによりリセットがトリガーされた (Reset triggered due to HA policy of Reset)」という理由で予期しないリロードが発生していた |
| CSCwa69303 | SSP プラットフォームで実行されている ASA で、重大なエラー「[FSM:FAILED]: sam:dme:MgmtIfSwMgmtOobIfConfig」が生成される                       |
| CSCwa76822 | syslog-ng 宛先のスロットリングフロー制御が調整される  |
| CSCwa77777 | ウォッチドッグインフラにログを追加  |
| CSCwa82850 | ASA フェールオーバーで、参加ノードを「スタンバイ準備完了」と宣言する前にコンテキストの不一致が検出されない  |
| CSCwa85297 | マルチインスタンス内部ポートチャネル VLAN が正しくプログラムされず、トラフィックが失われる   |
| CSCwa90735 | FTD/FXOS : ASAconsole.log ファイルのローテーションに失敗し、/ngfw で過剰なディスク容量が使用される  |
| CSCwa96920 | プロセス Lina で ASA/FTD がトレースバックおよびリロードすることがある   |
| CSCwa99171 | 再起動後に、シャーシとアプリケーションの時間が 2010 年 1 月 1 日に設定される   |
| CSCwa99932 | クラッシュおよび再起動後に ASA/FTD がスタックする  |
| CSCwb00871 | ENH : 拡張時またはストレス時のウォッチドッグを減らすために log_handler_file の遅延を削減   |

| ID         | 見出し   |
|------------|---|
| CSCwb01633 | モジュールの show-tech ファイル生成エラーの根本原因を診断するためのログが FXOS にない               |
| CSCwb02689 | FXOS は、NTP サーバーのローカルクロックストラタムではなく、参照クロックストラタムをチェックする必要がある         |
| CSCwb03704 | ASA/FTD データパススレッドがデッドロックに陥り、トレースバックを生成することがある                     |
| CSCwb04000 | ASA/FTD : VTI にルーティングされるパケットに DF ビットが設定されている                      |
| CSCwb05148 | Cisco ASA ソフトウェアと FTD ソフトウェアの SNMP におけるサービス妨害攻撃に対する脆弱性            |
| CSCwb18602 | crontab -e でエディタが見つからない   |
| CSCwb22359 | 誤った再起動とイベントのログ記録の増加を防ぐことを目的としたポートマネージャ/LACP の改善                   |
| CSCwb25809 | シングルパス : 古い ifc が原因でトレースバック                                       |
| CSCwb27099 | FXOS : Ciena Waveserver と Firepower シャーシ間におけるサードパーティとの相互運用。       |
| CSCwb28123 | 「デバイスのメジャーバージョンが変更されたため、展開に失敗した」というエラーで FTD HA 展開が失敗する            |
| CSCwb31551 | インバウンドパケットに SGT ヘッダーが含まれている場合、FPR2100 が 5 タプルごとに適切に配布できない         |
| CSCwb40662 | ENH : FCM に、インターフェイスの「リンクデバウンス時間」を変更するためのオプションを含める必要がある           |
| CSCwb48166 | 2.11 への FXOS アップグレードがスタックする                                       |
| CSCwb57524 | FTD アップグレードの失敗 : 配布可能パーティションの古い FXOS バンドルから十分なディスク容量を得られない        |
| CSCwb57615 | 行番号を使用した pbr アクセスリストの設定に失敗した。                                     |
| CSCwb57988 | smConLogger トレースバックは、メモリリークによって引き起こされる。                           |
| CSCwb58007 | CVE-2022-28199 : FTDv および ASA の評価                                 |
| CSCwb62059 | アップグレード後に外部認証を使用して FTD にログインできない                                  |
| CSCwb63827 | Cisco 適応型セキュリティアプライアンスと Firepower Threat Defense ソフトウェアの DoS の脆弱性 |

| ID         | 見出し  |
|------------|--|
| CSCwb66382 | ASAv : 9344 ジャンボフレームを有効にした後にブロックが自動的に作成されず、OSPF MD5 が壊れる                 |
| CSCwb70030 | MIO : 障害のシビラティ (重大度) が重大でない場合、または CATERR センサーが異なる場合、CATERR 中にブレードが再起動しない |
| CSCwb73678 | FXOS の /var/tmp パーティションのフルネスの警告  |
| CSCwb74498 | Cisco FXOS および NX-OS ソフトウェアの CDP DoS と任意のコード実行の脆弱性                       |
| CSCwb82796 | IKE トンネルを切断すると、ASA/FTD ファイアウォールがトレースバックおよびリロードすることがある                    |
| CSCwb83691 | FMC から開始されたキャプチャが原因で ASA/FTD のトレースバックとリロードが発生する                          |
| CSCwb88090 | FXOS : fxos config インポート後に新しいポートチャネルを作成すると、既存のポートチャネルがフラップする             |
| CSCwb90074 | ASA : マルチコンテキスト混合モード SFR リダイレクションの検証                                     |
| CSCwb95787 | FPR1010 : portmanager DIED イベント後、スイッチポート VLAN インターフェイスに ARP がない          |
| CSCwc02133 | Cisco FXOS ソフトウェアおよび Cisco FXOS ソフトウェアのコマンドインジェクションの脆弱性                  |
| CSCwc08683 | FPR1150 で光ファイバを抜いても、インターフェースの LED が緑色に点滅したままになる                          |
| CSCwc10145 | FTDv クラスタユニットがクラスタに再参加せず、エラーメッセージ「NLP SSL リスニングソケットを開けませんでした」が表示される      |
| CSCwc12652 | 9.18(1) または 7.2.0-82 Firepower にアップグレード後、コントロールプレーン ACL が機能しない           |
| CSCwc13017 | ./inspect/proxy.h:439 で FTD/ASA のトレースバックとリロードが発生する                       |
| CSCwc27846 | アップグレードおよびリロード後の HA 同期中に QP(multicontext)-99.18(28)9 でクラッシュが発生する         |
| CSCwc28806 | プロセス名 Lina で ASA がトレースバックし、リロードする  |
| CSCwc31457 | クリアテキストトークンを使用した ASA プロセス (暗号化できない場合)                                    |
| CSCwc37061 | SNMP : FMC が OID 1.3.6.1.2.1.25.3.3.1.2 に応答しない                           |
| CSCwc38361 | Cisco FXOS ソフトウェアのコマンドインジェクションの脆弱性                                       |

| ID         | 見出し  |
|------------|--|
| CSCwc40352 | Lina NetFlow から許可されたイベントが Stealthwatch に送信され、後で Snort によってブロックされる                              |
| CSCwc44289 | FTD : IPv4 <> IPv6 NAT 変換を実行するときのトレースバックとリロード  |
| CSCwc48375 | インバウンド IPSEC SA が非アクティブのままスタックする : 「show crypto ipsec sa」の1つのアウトバウンド SPI に対して多数のインバウンド SPI がある |
| CSCwc50887 | FTD : CCL リンク経由でリダイレクトされる UDP フローの NAT IPv4 <> IPv6 でのトレースバックとリロード                             |
| CSCwc50891 | MPLS タギングが FTD によって削除される   |
| CSCwc61106 | FXOS の cfg-export-policy で domain\username を設定できない   |
| CSCwc67687 | ASA HA フェールオーバーによって HTTP サーバーの再起動の失敗と ASDM の停止がトリガーされる   |
| CSCwc70962 | FTD/ASA の「書き込みスタンバイ」により ECDSA 暗号が有効になり、AC SSLv3 ハンドシェイクが失敗する                                   |
| CSCwc73209 | DOC : デフォルトのキーリングが FXOS 上の FCM によってのみ使用される   |
| CSCwc77519 | FPR1120-ASA : リロード後にプライマリがアクティブロールになる  |
| CSCwc77680 | ASA/FTD がスレッド名「DATAPATH-0-4948」でトレースバックおよびリロードすることがある  |
| CSCwc77892 | 起動後の ASA syslog の CGroups エラー  |
| CSCwc80234 | アクティブとスタンバイ間の「inspect snmp」設定が異なる  |
| CSCwc88897 | DNS インスペクションポリシー変更後の Cisco Umbrella のヌルポイントが原因で ASA がトレースバックおよびリロードする                          |
| CSCwc90091 | ユーザー統計がある ASA 9.12(4)47 が、「policy-server xxxx global」の可視性に影響する                                 |
| CSCwc94466 | Cisco ASA/FTD Firepower 2100 SSL/TLS におけるサービス妨害攻撃に対する脆弱性                                       |
| CSCwc99242 | リロード後に ISA3000 LACP チャネルメンバー SFP ポートが中断状態になる   |
| CSCwd00778 | SNMP ポーリングによる ifAdminStatus の出力が異常   |
| CSCwd03793 | FTD トレースバックとリロード   |



| ID                         | 見出し  |
|----------------------------|--|
| <a href="#">CSCwd05756</a> | syslog コンポーネントによる Lina の FTD トレースバック                 |
| <a href="#">CSCwd22349</a> | ASA : 「定期認証証明書」が有効になっている AnyConnect 証明書ベースの認証に接続できない |
| <a href="#">CSCwd31960</a> | カスタム NAT が設定されている場合、VPN 経由の管理アクセスが機能しない              |
| <a href="#">CSCwd40260</a> | 有用性の強化 : ペイロードを解析できない場合、ASA/FTD によってサイレントにドロップされる    |
| <a href="#">CSCwd51757</a> | 接続レート OID の SNMP GET を使用してポーリング結果を取得できない             |

## エンドユーザーライセンス契約書

エンドユーザーライセンス契約書の詳細については、<http://www.cisco.com/jp/go/warranty> にアクセスしてください。

## 関連資料

ASA の詳細については、『[Navigating the Cisco Secure Firewall ASA Series Documentation](#)』を参照してください。

---

【注意】 シスコ製品をご使用になる前に、安全上の注意（[www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。